

активами. Зрештою, розуміння взаємозв'язку між відомостями та даними в інформаційному праві вимагає вирішення глибоких філософських питань про природу реальності, межі людського розуміння та етичні імперативи справедливості та підзвітності. Це вимагає нюансованого підходу, який визнає складність і невизначеність, притаманні навігації в постійно розширюваному інформаційному ландшафті в правових контекстах.

#### Список використаних джерел:

1. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/2297-17> (дата звернення: 07.02.2024)
2. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/2939-17> (дата звернення: 07.02.2024)
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/go/2657-12> (дата звернення: 07.02.2024)

#### **Брулевич В. В.**

кандидат юридичних наук  
Державний біотехнологічний університет  
E-mail: [vova\\_brulevich@ukr.net](mailto:vova_brulevich@ukr.net)

### **ЗАХИСТ ВІД КІБЕРЗЛОЧИННОСТІ ТА ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ В ЦИФРОВІЙ СФЕРІ**

Сучасне суспільство відзначається швидким розвитком інформаційних технологій, що змінює не лише економічні та соціальні аспекти, але й ставить під сумнів звичайні уявлення про права, свободи та безпеку людини. Захист прав та свобод в інформаційній сфері стає надзвичайно важливим завданням, яке потребує комплексного підходу та системних заходів.

Один із основних викликів - це збереження приватності та захист персональних даних в інтернеті. За відсутності відповідних правових та

технічних механізмів, інформація про особу може стати об'єктом незаконного збирання, використання та поширення.

Міжнародним нормативно-правовим актом у сфері захисту персональних даних у мережі інтернет згода на обов'язковість застосування якого надана Верховною Радою України, є Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). [1]

Розробники цього документа наголошують: «Стрімкий технологічний розвиток і глобалізація призводять до виникнення нових труднощів для захисту персональних даних. Масштаби збирання та спільного використання персональних даних суттєво зросли. Технології дозволяють як приватним компаніям, так і публічним органам користуватися персональними даними в безпрецедентних масштабах з метою реалізації своєї діяльності. Фізичні особи дедалі частіше надають доступ до персональної інформації для громадськості та в глобальному масштабі. Технології змінили як економіку, так і суспільне життя і повинні надалі стимулювати вільний рух персональних даних у межах Союзу та передавання їх до третіх країн і міжнародних організацій, забезпечуючи при цьому високий рівень захисту персональних даних. Такі зміни вимагають наявності міцних та більш узгоджених засад щодо захисту даних у Союзі, із запровадженням належного механізму виконання, беручи до уваги важливість формування довіри, що дозволить розвиток цифрової економіки на рівні внутрішнього ринку. Фізичні особи повинні мати контроль щодо власних персональних даних. [2, с. 23]

До основних проблем можна віднести: недостатній контроль над персональними даними, ризик порушення конфіденційності, проблеми з правовим регулюванням.

**Способи вирішення.** 1. Просвітництво та освіта: Забезпечення користувачів інтернету достовірною та доступною інформацією щодо захисту їхніх персональних даних. 2. Створення сильних стандартів безпеки: Підвищення вимог до організацій, що збирають та обробляють персональні дані, з метою забезпечення їх безпеки та конфіденційності. 3. Розвиток технологічних рішень: Використання криптографії, блокчейн технологій та інших інноваційних підходів для захисту даних в Інтернеті. 4. Законодавчі заходи: Удосконалення законодавства щодо захисту персональних даних та введення суворих штрафних санкцій за їх порушення.

Другий виклик полягає в боротьбі з кіберзлочинністю. У зв'язку зі зростанням кількості та складності кібератак, необхідно приймати ефективні заходи для захисту інформаційних ресурсів та запобігання кіберзлочинам.

Одне з найбільш ґрунтовних діянь, зорієнтованих на регулювання цієї проблеми, є ухвалення Рекомендацією Європи 23 листопада 2001 р. Конвенції про кіберзлочинність (ратифікована 1 липня 2004 р.).

Конвенція про кіберзлочинність представляється первинною міжнародною угодою у сфері протидії правопорушенням, вчиненим посередництвом комп'ютера. В рамках одинадцятого і дванадцятого Конгресів організації щодо запобігання злочинності та кримінального правосуддя (UN Congress on Crime Prevention and Criminal Justice) обговорювалися проблемні проблеми інтернаціонального партнерства у війні з кіберзлочинністю. Члени Конгресів обговорювали заходи щодо інтенсифікації інтернаціонального партнерства і поліпшення державного законодавства у галузі боротьби з відмиванням коштів, торгівлі наркотиками, тероризмом та кіберзлочинністю. Тобто, ООН встановила комп'ютерні правопорушення в єдиний цикл з тероризмом, що вказує на

спеціальний інтерес до даного питання зі сторони світової спільноти. [3, с. 388]

Законом України «Про основні засади забезпечення кібербезпеки України» 2017 року визначено правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. У законі поняття «кіберзлочин» («комп'ютерний злочин») трактується як суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України, а кіберзлочинність визначено як сукупність кіберзлочинів. [4]

Водночас тенденції розвитку суспільних відносин в Україні протягом останніх років демонструють такі найбільш поширені кіберзлочини: кібершахрайство з метою заволодіння коштами; кібершахрайство з метою заволодіння інформацією (для власного користування або для подальшого продажу); втручання в роботу інформаційних систем із метою одержання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для нанесення збитків конкурентам); інші злочини. [5, с. 121]

**Способи вирішення.** 1. Штучний Інтелект та Машинне Навчання: Використання штучного інтелекту та машинного навчання дозволяє створювати більш ефективні та автоматизовані системи виявлення та запобігання кіберзлочинності. 2. Квантові Технології: Розвиток квантових технологій може привести до створення надійних систем шифрування, які забезпечать більшу захищеність персональних даних. 3. Глобальні

Стандарти: Розробка та впровадження глобальних стандартів у сфері кібербезпеки сприятиме більш ефективній боротьбі з кіберзлочинністю на міжнародному рівні.

Отже, аналізуючи вище викладене, можна констатувати, що боротьба з кіберзлочинністю та захист персональних даних є критично важливим завданням у сучасному цифровому світі. Розвиток нових технологій, таких як штучний інтелект та квантові технології, а також впровадження глобальних стандартів кібербезпеки, відіграють важливу роль у забезпеченні захисту від кіберзлочинності та забезпеченні безпеки персональних даних. Тільки завдяки поєднанню зусиль урядових структур, приватного сектору та громадськості можна досягти значного прогресу в цій сфері та забезпечити безпеку в цифровому середовищі для всіх користувачів.

#### **Список використаних джерел:**

1. Регламент Європейського Парламенту і Ради (ЄС) 216/679 від 27.04.2016 р. про захист фізичних осіб при обробці персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: <https://ips.ligazakon.net/document/MU16144> (дата звернення 08.04.2024)
2. Бліхар М. М. Правові основи захисту персональних даних в інтернеті. Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2023 № 62. С. 20-24
3. Саєнко М.І., Савела Є.А., Тополянський Ю.Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. 2021 Випуск 64 С. 386-391
4. Про основні засади забезпечення кібербезпеки України: Закон України від 5.10.2017. URL: <http://zakon5.rada.gov.ua/laws/show/2163-19>.
5. Шемчук В.В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. 2018 Том 29 (68) № 6 С. 119-124